Systemic Risk in Networks

Nils Detering[*], Thilo Meyer-Brandis[†], Konstantinos Panagiotou[†], Daniel Ritter[†]

April 4, 2019

Abstract

Systemic risk, i.e. the risk that a local shock propagates throughout a given system due to contagion effects, is of great importance in many fields of our lives. In this summary article we show how asymptotic methods for random graphs can be used to understand and quantify systemic risk in networks. We define a notion of resilient networks and present criteria that allow us to classify networks as resilient or non-resilient. We further examine the question how networks can be strengthened to ensure resilience. In particular, for financial systems we address the question of sufficient capital requirements. We present the results in random graph models of increasing complexity and relate them to classical results about the phase transition in the Erdös-Rényi model. We illustrate the results by a small simulation study.

Keywords: systemic risk, financial contagion, capital requirements, inhomogeneous random graphs, weighted random graphs, directed random graphs

1 Introduction

One possible attempt to define *Systemic Risk* is that in case of an adverse local shock (infection) to a system of interconnected entities a substantial part of the system, or even the whole system, finally becomes infected due to contagion effects. In an evermore connected world systemic risk is an increasing threat in many fields of our life, examples include the epidemic spread of diseases, the collapse of financial networks, rumor spreading in social networks, computer viruses infecting servers or breakdowns of power grids. However, as for example the recent financial crisis has demonstrated, traditional risk management strategies and techniques often only inadequately account for systemic risk as they predominantly focus on the single system entities and only insufficiently consider the whole system with its potentially devastating contagion effects. It is thus of great interest to develop new quantitative tools that can support the process of identifying, measuring, and managing systemic risk. This problem has been addressed in a number of papers now and the literature is still growing. One active line of research is the extension of the axiomatic approach to monetary risk measures from Financial Mathematics, initiated in [7], to systemic risk measures, see e. g. [11, 30, 24, 25, 8, 19, 6]. Another interesting analysis of systemic risk is based on an explicit modeling of the underlying network of interacting entities and potential contagion effects, see [17, 22, 31, 3, 32, 12]. For a further overview of different methods and concepts to address systemic risk, the reader is referred to the two monographs [20] and [27]. In this chapter, we give an account of how such tools can be developed

[*]Department of Statistics and Applied Probability, University of California, Santa Barbara, CA 93106, USA. Email: detering@pstat.ucsb.edu

[†]Department of Mathematics, University of Munich, Theresienstraße 39, 80333 Munich, Germany. Emails: meyerbra@math.lmu.de, kpanagio@math.lmu.de and ritter@math.lmu.de

for large networks in the framework of random graph models, which allows both for an explicit modeling of the underlying network structure as well as of the contagion process propagating systemic risk. This area of research has been initiated by the work [21], [2] and further developed in [15] and [16].

For a system with n entities (nodes) with labels in $[n] := \{1, \dots, n\}$, rather than dealing with a specific deterministic network we consider a random graph model G on a given probability space $(\Omega, \mathcal{F}, \mathbb{P})$, where for each scenario $\omega \in \Omega$ the realized network is represented by its adjacency matrix $G(\omega) \in \{0,1\}^{n \times n}$. We want to exclude self-loops from the graph and hence assume $G_{i,i} = 0$ almost surely for all $i \in [n]$. Further, if we consider undirected networks, then $G_{i,j}(\omega) = G_{j,i}(\omega)$ for all $i, j \in [n]$. If $G_{i,j}(\omega) = 1$, then we say that (i, j) is an edge of G.

The motivation for choosing such a random graph framework is twofold. From a modeling point of view, risk management deals with the uncertainty of adverse effects at a future point in time. In many situations, however, not only the future adverse shock is uncertain but also the specific network structure. While the statistical characteristics (degree distribution, ...) of the considered network often remain stable over time, the specific configuration of edges may change. This uncertainty is then represented by a suitable random graph model. Secondly, from a mathematical point of view, the framework of random graphs allows for the application of the law of large number effects when the network size gets large. This enables the analytic derivation of asymptotic results that hold for all "typical" future realizations $G(\omega)$ of large networks (more precisely, the results hold *with high probability* (w. h. p.), that is with probability growing to 1 when n tends towards infinity). In this sense our systemic risk management results are robust with respect to the uncertainty about the future network configuration and applicable to all "typical" networks that share the same statistical characteristics.

The random graph models we consider are characterized by the fact that each possible edge e is included *independently* with some probability p_e. Our models differ in the way the marginal probabilities are actually specified: if all p_e are equal, then we call this the *homogeneous* setting. This is the classical Erdös-Rényi model. We refer the reader to [9, 1, 28] for an excellent introduction to the model and its asymptotic properties. All other cases are called *heterogeneous* and the resulting model is often called the inhomogeneous random graph in the literature. In the latter case the actual degree of heterogeneity has an important effect on several structural characteristics of the resulting graphs (as for example the distribution of the edges in the graph, or the emergence of a core-periphery structure), and we will exploit this effect to capture realistic situations. The recent monograph [26] gives an extensive introduction to this heterogeneous model and its alternatives including the configuration model.

In addition to the specification of a random graph model, we explicitly model the contagion effects by which an initial local shock propagates throughout the system. The contagion processes we consider in this chapter are generalizations of the so-called *bootstrap percolation process*. The essential feature specifying the contagion process is the assumption that each node i is equipped with a threshold value $\tau_i \in \mathbb{N}$ that represents the "strength" of node i to withstand contagion effects. Given a subset $I \subset [n]$ of initially "infected" nodes, the contagion process can then be described in rounds where node $i \in [n]$ gets infected as soon as τ_i of its neighbors are infected. This contagion process then clearly ends after at most $n-1$ rounds leading to the set of eventually infected nodes triggered by the initially infected nodes I. The essential risk indicator underlying our analysis of systemic risk is then the *final infection fraction*

$$\alpha_n := \frac{\text{number of finally infected nodes}}{n} \tag{1.1}$$

given by the number of finally infected (or defaulted) nodes triggered by the set I of initially infected nodes divided by the total number of nodes in the network.

When such a contagion process is studied on a random graph G, the final default fraction $\alpha_n(\omega)$ is a random variable that depends on the realized network $G(\omega)$, and the first main question is whether one can quantify the final default fraction. Asymptotically for large networks this question can be answered positively for the random graph models we consider, and we show that the final default fraction is given by some deterministic, analytic formula depending on the statistical network characteristics and the contagion process in the limit in probability as $n \to \infty$. So roughly speaking, when the network size n is large enough, the final default fraction can be computed analytically and it will be the same for almost all network realizations $G(\omega)$ of the random graph G (and in this sense is robust with respect to the uncertainty about the future network structure).

Based on the analysis of the final default fraction we then develop a quantitative concept to asses the systemic riskiness of a network. More precisely, we present a mathematical criterion formulated in terms of the network statistics that characterizes whether a network is resilient or non-resilient with respect to initial shocks. Roughly speaking, a network is resilient, and thus acceptable from a systemic risk point of view, if small shocks remain small, and it is non-resilient, and thus non-acceptable from a systemic risk point of view, if any initial shock propagates to a substantial part of the system, no matter how small the initial shock is. We will see that in terms of this resilience criterion the systemic riskiness of a network heavily depends on the topology of the graph. In particular, as long as the degree sequence possesses a second moment only local effects determine whether a network is resilient or not and the absence of so-called contagious edges in the network guarantees resilience. Here, an edge (i, j) is called *contagious* if the mere infection of node j leads to the infection of node i (or vice versa). If, on the other hand, the degree sequence has infinite second moment, a property that many real world networks share, many global effects contribute to the contagion process and the absence of contagious links no longer implies resilience.

Once a measure of systemic risk is introduced, the second important question is how to manage systemic risk, i. e., how to design or control a system such that it is acceptable from a systemic risk point of view. In our framework we analyze this question in the following sense: For a given graph structure, how does one have to specify the threshold values τ_i, $i \in [n]$, such that the network becomes resilient? For example in the context of financial networks, requirements on τ_i can be interpreted as capital requirements imposed on a financial institution $i \in [n]$. Using above mentioned resilience criterion, it follows immediately that for networks with finite second moment of the degree sequence the requirement $\tau_i \geq 2$, $i \in [n]$, is sufficient for resilience since this excludes contagious edges. For networks without finite second moment of the degree sequence this management rule is insufficient for securing a system and we will see that highly connected nodes need to be equipped with higher threshold values. In particular, we will characterize resilience/non-resilience in terms of a specific functional form for the threshold values, where the threshold value τ_i for node i can still basically be determined locally by only knowing the profile of node i. This striking feature is possible due to averaging effects in large random graphs and it is in contrast to other management (or allocation) rules obtained in deterministic networks that for each node can only be specified in terms of the complete network structure.

In the course of this chapter we expose the program sketched above in gradually increasing complexity of both the underlying random graph model and the contagion process. In Section 2.1, we consider the homogeneous setting of the well-studied Erdös-Rényi random graph and the classical bootstrap percolation process with constant threshold values. In Section 2.2, to account for more realistic features of many empirically observed networks, we extend the homogeneous setting to both heterogeneous random graphs and threshold values, which in particular allows for graphs with infinite second moment degree sequences. Finally, in Section 2.3,

we focus on the modeling of financial networks where the contagion process is driven by capital endowments and exposures of the financial institutions. This contagion process represents a further extension/generalization of the threshold-driven contagion process. The results of both Sections 2.2 and 2.3 were originally derived in [15, 16]. It is the aim of this chapter to summarize this work and make our results comprehensible to a broad audience of different backgrounds.

2 Models of networks and contagion processes

In this section we will describe various models of random networks and contagion processes, accompanied by several results characterizing their qualitative behavior. The presentation will be such that the complexity of both the considered networks models, as well as the contagion process, increases gradually from a rather homogeneous setting to one that may resemble some realistic situations quite well.

Random Graph Models Our random graph models have the following common characteristics. We assume that a number n of nodes with labels in $[n] := \{1, \dots, n\}$ is given. The set of possible edges E_n consists then either of all unordered pairs $\{i, j\}$, where $i \neq j$ ("undirected graph") or all ordered pairs (i, j), where again $i \neq j$ ("directed graph"). The graph G is specified by including each possible edge e *independently* with some probability p_e. Our models differ in the way the marginal probabilities $(p_e)_{e \in E_n}$ are actually specified: if all p_e are equal, then we call this the homogeneous setting, and all other cases are called heterogeneous. In the latter case the actual degree of heterogeneity has an important effect on several structural characteristics of the resulting graphs (as for example the distribution of the edges in the graph, or the emergence of a core-periphery structure), and we will exploit this effect to capture realistic situations.

Contagion Processes The contagion processes that we consider here resemble and extend the well-studied *bootstrap percolation* process, which has its origin in the physics literature [10]. In the classical setting a graph G is given and initially a subset I of the nodes is declared *infected*. We will make the assumption that each node is initially infected with some probability $\epsilon > 0$, independently of all other nodes. The process then consists of rounds, in which further nodes may get infected. Similar as with the random graph also the infection rules that we study will become gradually more complex to represent more realistic settings. We start with the simple rule 1BP where a node becomes infected as soon as one of its neighbors becomes infected. More complex rules we study then allow for variation in the nodes' individual infection thresholds (for example, rBP stands for the rule in which each node has threshold r) and the impact of different edges. More concrete rules will be introduced later. In all cases we will be interested in the size of the set of eventually infected nodes. For each finite graph size n this is a random number which depends on the realized graph configuration. However, due to averaging effects we will be able to compute the (random) fraction of eventually infected nodes $\alpha_n(\epsilon)$ as in (1.1) as a deterministic number $\alpha(\epsilon)$ in the limit $n \to \infty$ under some mild regularity assumptions.

Resilience to Contagion For many applications the spread of the initially infected set to the whole graph is of central importance. In some cases it may be favorable if a small fraction ϵ of initially infected nodes spreads to a large fraction of the whole graph; in other cases such behavior would be rather worrisome. To capture these two different kinds of possible behavior, we give the following definitions:

Definition 2.1. A network is said to be *resilient* if $\alpha(\epsilon) \to 0$ as $\epsilon \to 0$.

Definition 2.2. A network is said to be *non-resilient* if there exists some lower bound $\underline{\alpha} > 0$ such that $\alpha(\epsilon) > \underline{\alpha}$ for all $\epsilon > 0$.

Definition 2.1 characterizes a network as being resilient (to small initial infections) if the final fraction of infected nodes vanishes as the fraction of initially infected nodes ϵ tends to 0. In this case, small local shocks cannot cause serious harm to the system but they only impact their immediate neighborhood in the graph. On the other hand, Definition 2.2 classifies networks as non-resilient if every howsoever small initial fraction $\epsilon > 0$ causes a positive fraction of at least $\underline{\alpha} > 0$ of eventual infections. In particular, the amplification factor $\alpha(\epsilon)/\epsilon$ explodes as ϵ becomes small and the effects are not locally confined anymore.

2.1 Homogeneous setting

In this section we study the homogeneous setting which comprises three assumptions. First, the graph is undirected, i. e. we have n nodes and the set of possible edges is $E_n := \binom{[n]}{2} = \{\{i, j\} : 1 \leq i, j \leq n, i \neq j\}$. Second, for every $e \in E_n$ we assume that $p_e = p$, that is, the probability that an edge is present is the same for all edges. This is a classical and well-studied model of random graphs that was first introducted in [23, 18] and it has been investigated in great detail since then, see [9] for an excellent introduction. Our third and final assumption is that in the contagion process all nodes are initially infected with the same probability ε and the infection thresholds are also equal to some number $r \in \mathbb{N}$, which means that any node becomes infected as soon as (at least) r of its neighbors are infected. This infection process is well understood and treated in detail in [29] and all results in this section are either special cases of results in [29] or easily arise from them.

We shall use the standard notation $G_{n,p}$ for a random graph with n nodes and edge probability p as described in this section. For different choices of p this graph shows different characteristics and can range from a very sparse, loosely connected graph to a very dense graph. In particular, note that the number $e(G_{n,p})$ of edges in $G_{n,p}$ follows a binomial distribution with parameters $|E_n| = \binom{n}{2}$ and p. Thus, the expected number of edges in $G_{n,p}$ equals $\binom{n}{2}p$, and their actual number is typically close to this value. Here we will focus especially on the case $p = p(n) = c/n$ for some $c > 0$, as then $\mathbb{E}(e(G_{n,p})) = \frac{c}{2}(n-1) \sim cn/2$, a quantity that is linear in the number of nodes and thus most interesting for the applications that we have in mind. See Figure 1 for an illustration of such a network.

A well-known structural property of the random graph $G_{n,c/n}$ that will become quite handy later is that, as $n \to \infty$, the (random) degree $\deg(i)$ of each node $i \in [n]$ converges weakly to a Poisson distribution with parameter c. Furthermore, if one considers the (random) empirical degree distribution

$$\tilde{F}_n(k) := n^{-1} \sum_{i \in [n]} \mathbf{1}\{\deg(i) \leq k\}, \quad k \in \mathbb{N}_0$$

then the following statement is true (see for example [26, Theorem 5.12]):

Lemma 2.3. *As $n \to \infty$, $\tilde{F}_n$ converges to a Poisson distribution with parameter c.*

After having introduced the underlying random graph model for this section, we are now interested in analyzing the contagion mechanism. Recall that regarding the contagion process we assume that each node is infected initially with some probability $\varepsilon > 0$ and independently of all other nodes. Nodes that are not initially infected shall become so as soon as $r \in \mathbb{N}$ of their neighbors are infected, i. e. $\tau_i = r$ for all nodes $i \in [n]$ that are not infected initially. In the sequel we distinguish the cases $r = 1$ and $r \geq 2$ for the infection threshold of each node. Our main focus will be to distinguish between two fundamentally different behaviors:

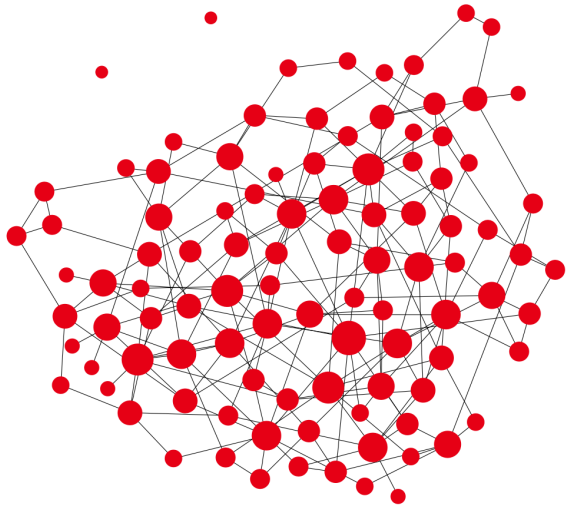


Figure 1: A typical configuration for $G_{n,p}$ with $n = 100$, $c = 4$ and $p = c/n$. Node sizes scale with the corresponding degree.

$\mathbf{r = 1}$*:* Observe that in this case a node gets infected as soon as any of its neighbors is infected. In particular, if i is a node that was infected at the beginning of the process, then eventually the whole connected component containing i will become infected; hence the behavior of the process is intimately related to the component structure of $G_{n,p}$. Here, the famous result of Erdös and Rényi (see [1] for example) regarding a phase transition in the component structure comes to help. Let us write $L(G_{n,p})$ for the random number of nodes in a largest connected component of $G_{n,p}$.

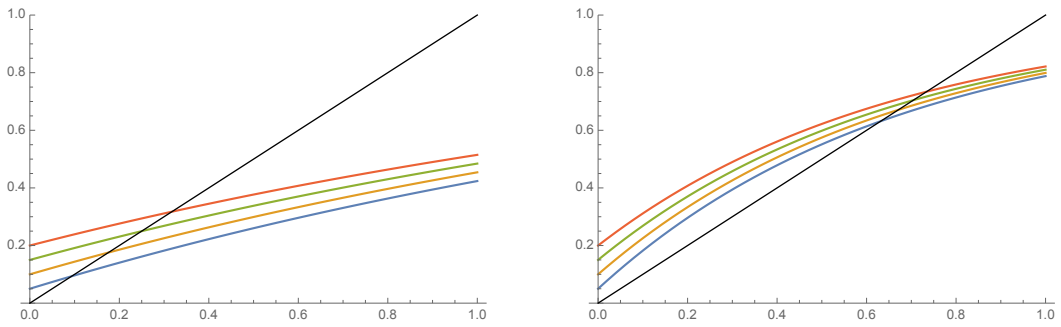
Theorem 2.4. *Let $c > 0$ and $p = c/n$. Then, as $n \to \infty$,*

- *if $c < 1$, then there exists $\kappa \in (0, \infty)$ such that $\log^{-1}(n) L(G_{n,p}) \to \kappa$ in probability.*
- *if $c > 1$, then there exists $\lambda \in (0, \infty)$ such that $n^{-1} L(G_{n,p}) \to \lambda$ in probability.*

A first important consequence of this result is that if $c > 1$, then, no matter how small $\varepsilon > 0$ is chosen, w. h. p. (i. e. with probability converging to 1 as $n \to \infty$) at least one node in the largest component will be infected and in turn at least a fraction λ of the nodes in the graph will eventually become infected. We hence derive the following result:

Theorem 2.5. *Consider the random graph model $G_{n,p}$ with $p = c/n$ and threshold $r = 1$. If $c > 1$, then the system is non-resilient.*

Regarding the case $c < 1$ it turns out that $G_{n,c/n}$ is resilient according to Definition 2.1. We do, however, need more information about the random graph than only the size of its largest component in order to conclude this. Indeed, from a heuristic point of view, the following consideration is helpful: Let $\alpha(\epsilon) \in [\epsilon, 1]$ be the (a priori possibly random) fraction of eventually infected nodes. Each of the eventually infected nodes is either infected from the beginning, which happens with probability ϵ, or otherwise it must have at least one infected neighbor. We know that the degree of each node is Poisson distributed with mean c in the limit $n \to \infty$. Since a fraction $\alpha(\epsilon)$ of all nodes is eventually infected, for each node i that becomes infected during the



(a) (b)

Figure 2: Plot of f_ϵ for $\epsilon \in \{0.05, 0.1, 0.15, 0.2\}$ and $c = 0.5$ (a) respectively $c = 1.5$ (b). In black the diagonal $h(z) = z$.

process (not initially infected) the number of infected neighbors can be expected to be Poisson distributed with parameter $c\alpha(\epsilon)$. This heuristic argument yields the identity

$$\alpha(\epsilon) = \epsilon + (1 - \epsilon)\mathbb{P}(\text{Poi}(c\alpha(\epsilon)) \geq 1)$$

The fraction $\alpha(\epsilon)$ should then be a fixed point of the function

$$f_\epsilon(z) := \epsilon + (1 - \epsilon)\mathbb{P}(\text{Poi}(cz) \geq 1).$$

Since f_ϵ is continuous, $f_\epsilon(0) = \epsilon > 0$, and $f_\epsilon(1) \leq \epsilon + (1 - \epsilon) = 1$, there always exists at least one fixed point of f_ϵ within $(0, 1]$. Further, since $f''_\epsilon(z) = -c^2(1 - \epsilon)e^{-cz} < 0$ for all $z \in [0, \infty)$, there can only exist one solution $\hat{z}$ to $f_\epsilon(z) = z$. This solution must hence coincide with the final fraction of infected nodes. Making this heuristic argument rigorous (compare to Theorem 2.8), we derive the following result.

Theorem 2.6. *Consider the random graph model $G_{n,p}$ with $p = c/n$ and threshold $r = 1$. Let $\hat{z}$ denote the unique fixed point of $f_\epsilon(z)$. Then the fraction of eventually infected nodes converges to $\alpha(\epsilon) = \hat{z}$ in probability.*

Regarding the case $c < 1$, note that as the initial infection probability $\epsilon \to 0$, the fixed point of $f_\epsilon(z)$ also converges to 0 since $f_\epsilon(z) \leq \epsilon + (1 - \epsilon)cz$ and hence $\hat{z} \leq \epsilon(1 - c)^{-1}$. See Figure 2(a) for an illustration. This means that the final fraction of infected nodes vanishes and the network is thus resilient according to Definition 2.1:

Theorem 2.7. *Consider the random graph $G_{n,p}$ with $p = c/n$ and threshold $r = 1$. If $c < 1$, then the system is resilient.*

On the other hand, for the case that $c > 1$ the fixed point of f_ϵ is lower bounded for all $\epsilon > 0$ which is in line with Theorem 2.5, see Figure 2(b).

r $\geq$ 2: Also in this case the same heuristic reasoning as for $r = 1$ shows that

$$\alpha(\epsilon) = \epsilon + (1 - \epsilon)\mathbb{P}(\text{Poi}(c\alpha(\epsilon)) \geq r)$$

for the fraction $\alpha(\epsilon)$ of eventually infected nodes. This time, however, it is possible in general that the function

$$f_\epsilon(z) := \epsilon + (1 - \epsilon)\mathbb{P}(\text{Poi}(cz) \geq r)$$

has one, two, or three different fixed points in $(0,1]$, depending on the values of c and ϵ. We can still describe the final infection fraction by choosing the smallest fixed point but we require an additional condition: A fixed point $\hat{z}$ of f_ϵ is called *stable* if $f'_\epsilon(\hat{z}) < 1$. The following result is then a special case of [29, Theorem 5.2.]:

Theorem 2.8. *Let $\hat{z}$ be the smallest fixed point of $f_\epsilon(z)$ in $(0,1]$ and assume that it is stable. Then the fraction of eventually infected nodes converges to $\alpha(\epsilon) = \hat{z}$ in probability.*

The theorem gives us a way to compute the final infection fraction for any given c and ϵ. In order to derive a statement about resilience of the network, note that $\mathbb{P}(\mathrm{Poi}(cz) \geq r) \leq \mathbb{P}(\mathrm{Poi}(cz) \geq 2) \leq (cz)^2/2$ and hence $f_\epsilon(z) \leq \epsilon + (cz)^2/2$. Thus the smallest fixed point $\hat{z}$ of f_ϵ is upper bounded by $(1 - \sqrt{1 - 2\epsilon c^2})c^{-2}$ which tends to 0 as $\epsilon \to 0$. Regardless of c we then obtain the following statement.

Theorem 2.9. *Consider the random graph model $G_{n,p}$ with $p = c/n$. If $r \geq 2$ (no contagious links), then the system is resilient.*

After having introduced our measure of systemic risk, we can now employ the resilience criteria formulated in Theorems 2.7 and 2.9 to derive the following management rules for the network thresholds to control systemic risk in the homogeneous random graph: In the case that $c < 1$, we do not need to impose any restrictions on the thresholds τ_i, $i \in [n]$. For the case that $c \geq 1$, it will be sufficient to require that $\tau_i \geq 2$ for all $i \in [n]$.

2.2 Getting heterogeneous

As a matter of fact, only few networks are homogeneous enough to be well described by an Erdös-Rényi random graph. Most networks exhibit a strong degree of heterogeneity. The aim in this section is to describe an enhanced random graph model that overcomes this issue. Further, we change from the undirected random graph $G_{n,p}$ to a directed one since many real world networks such as the network of interbank lending are directed. The model we present here was proposed in [15] and is a directed version of the Chung-Lu inhomogeneous random graph, see [13, 14]. The results presented in this section are special cases of results in [15, 16]. Notable earlier works on the contagion process $r\mathsf{BP}$ in an undirected inhomogeneous random graph can be found in [5, 4].

We begin with a detailed description of the random graph model. We assign to each node $i \in [n]$ two weights: an *in-weight* w_i^- and an *out-weight* w_i^+. The in-weight describes the tendency of i to develop in-coming edges (that is, edges pointing towards i), whereas the out-weight describes the tendency of developing out-going edges (that is, edges pointing away from i). To formalize this, define for each possible edge $e = (i,j)$ going from node $i \in [n]$ to $i \neq j \in [n]$ the edge probability p_e by

$$p_e := \min\{1, n^{-1} w_i^+ w_j^-\}. \tag{2.1}$$

We denote the resulting random graph by $G_n(\mathbf{w}^-, \mathbf{w}^+)$, where $\mathbf{w}^- := (w_1^-, \ldots, w_n^-)$ and $\mathbf{w}^+ := (w_1^+, \ldots, w_n^+)$. The heterogeneity of the graph stems from assigning different weights to different nodes. In order to make statements about the graph in the limit $n \to \infty$, it is required that the graph grows in a somehow regular fashion. In fact, we require that the fraction of nodes with weight level in any given interval stabilizes. To make this more precise define the empirical distribution function

$$F_n(x,y) := n^{-1} \sum_{i \in [n]} \mathbf{1}\{w_i^- \leq x, w_i^+ \leq y\}.$$

and let (W_n^-, W_n^+) be a random vector distributed according to F_n. We shall assume that (W_n^-, W_n^+) converges in distribution to some random vector (W^-, W^+), and that furthermore $\mathbb{E}[W_n^-] \to \mathbb{E}[W^-] =: \lambda^- < \infty$ and $\mathbb{E}[W_n^+] \to \mathbb{E}[W^+] =: \lambda^+ < \infty$.

The random vector (W^-, W^+) serves as a limit object that is stongly associated to the sequence of random graphs $G_n(\mathbf{w}^-, \mathbf{w}^+)$ for $n \in \mathbb{N}$. We will see that it fully determines the degrees of its nodes and the outcome of the contagion process. As for the homogeneous random graph $G_{n,p}$, also in the heterogeneous setting we can describe the degree of each node in the limit $n \to \infty$. This time, every node $i \in [n]$ has an in-degree $\deg^-(i)$ and an out-degree $\deg^+(i)$. As in the homogeneous setting, their distribution is based on a Poisson distribution but also the weights w_i^- and w_i^+ play a role. More precisely, for large network sizes n it holds that $\deg^-(i) \sim \mathrm{Poi}(w_i^- \lambda^+)$ and $\deg^+(i) \sim \mathrm{Poi}(w_i^+ \lambda^-)$. To reverse the logic, it can be shown that in- and out-degree of each node function as maximum-likelihood estimators of its in- and out-weight (up to normalizing factors) when we want to calibrate our model parameters to some observed network structure. One can thus basically think of the weights in our model as the realized degrees of each node. It is hence no surprise that also the whole degree sequence is intimately related to the weight distribution. Consider the (random) empirical degree distribution

$$\tilde{F}_n(k,l) = n^{-1} \sum_{i \in [n]} \mathbf{1}\{\deg^-(i) \leq k, \deg^+(i) \leq l\}.$$

For a two-dimensional random vector (X, Y) let $Z = (\mathrm{Poi}(X), \mathrm{Poi}(Y))$ denote a two-dimensional mixed Poisson random vector with probability mass function given by

$$\mathbb{P}\left(Z = \binom{k}{j}\right) = \mathbb{E}\left[e^{-(X+Y)} \frac{X^k Y^j}{k!\, j!}\right].$$

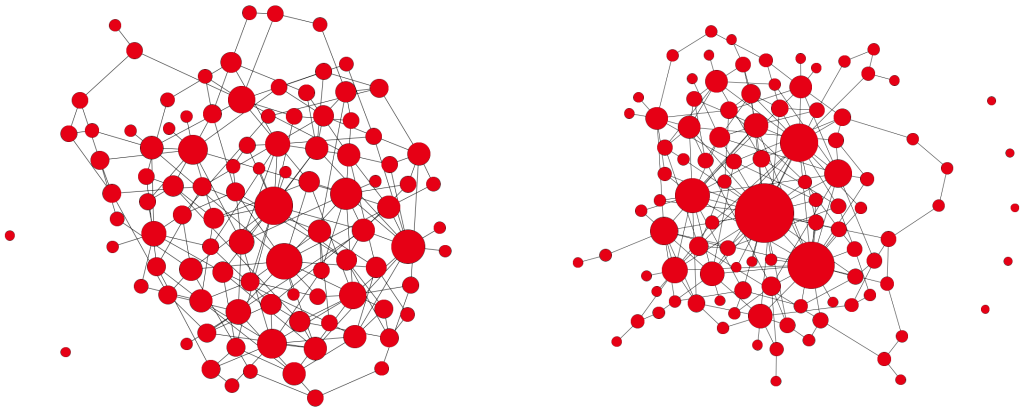
Then the degrees in the network are described as follows:

Lemma 2.10. *The (random) empirical in- and out-degree distributions over all nodes converge to the distribution of the random vector* $(\mathrm{Poi}(W^- \lambda^+), \mathrm{Poi}(W^+ \lambda^-))$.

In particular, $G_n(\mathbf{w}^-, \mathbf{w}^+)$ has much more flexibility in its degree distribution than $G_{n,c/n}$. By choosing weights W^- and W^+ with infinite variance it is even possible to describe networks whose degree distributions have unbounded second moment – a feature that is often observed in real networks. See Figures 3(a) and 3(b) for an illustration of the heterogeneity of $G_n(\mathbf{w}^-, \mathbf{w}^+)$. Also compare with Figure 1. All three figures show graphs with exactly 200 edges but differ in the realized degree sequences due to the different choices for the weight distributions.

For the description of the contagion process, note that in real networks not only the network topology is very heterogeneous, but also the strengths of the different nodes. In the previous section, we described the contagion process by $r\mathsf{BP}$. However, there might be nodes that can endure more defaults of their neighbors than others. Therefore, we assign an *individual* threshold $\tau_i \in \mathbb{N} \cup \{\infty\}$ to each node describing the number of neighbors of i that need to become infected before i becomes infected as well. For example, in a banking network, τ_i can be thought of as the capital of some bank i. Let similarly as before (W_n^-, W_n^+, T_n) be a random variable with distribution equal to the empirical distribution of the weights and thresholds and assume that also for the extended network, (W_n^-, W_n^+, T_n) converges in distribution to some random vector (W^-, W^+, T). Similar as in the previous section, under these mild assumptions it is then possible to determine the fraction of eventually infected nodes by computing the smallest fixed point of a certain function. For $\epsilon > 0$ let

$$f_\epsilon(z) := \epsilon \mathbb{E}[W^+] + (1-\epsilon)\mathbb{E}[W^+ \mathbb{P}(\mathrm{Poi}(W^- z) \geq T)],$$



(a) (b)

Figure 3: Typical configurations for $G_n(\mathbf{w}^-, \mathbf{w}^+)$ with $n = 100$ and Pareto-distributed weights with shape parameter (a) 3.5 (bounded second moment) respectively (b) 2.5 (unbounded second moment). For simplicity the graphs are depicted undirected. Node sizes scale with the corresponding degree.

which is clearly a continuous function. Since $f_\epsilon(0) = \epsilon$ and $f_\epsilon(\mathbb{E}[W^+]) \leq \mathbb{E}[W^+]$, there will always exist at least one fixed point $\hat{z}$ of f_ϵ within $(0, \mathbb{E}[W^+]]$. As before we call such a fixed point *stable* if f_ϵ is continuously differentiable at $\hat{z}$ with $f'_\epsilon(\hat{z}) < 1$. Then the following holds:

Theorem 2.11. *Let $\hat{z}$ be the smallest fixed point of f_ϵ and assume that it is stable. Then, the fraction of eventually infected nodes converges in probability to*

$$\alpha(\epsilon) = \epsilon + (1 - \epsilon)\mathbb{E}[\mathbb{P}(\mathrm{Poi}(W^- \hat{z}) \geq T)].$$

For the sake of readability we restrict ourselves to the typical case that $\hat{z}$ is stable in Theorem 2.11. For more general results see [15, 16].

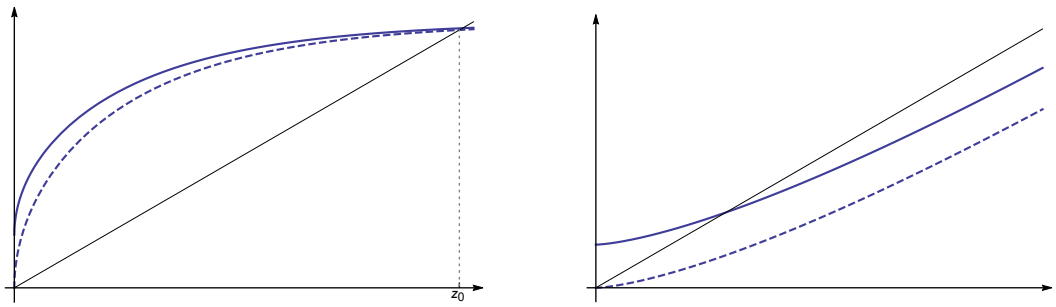
Having quantified the final infection fraction we can then turn our attention to investigating the resilience properties of the generalized heterogeneous networks. These are intimately related to the behavior of $f_0(z)$ near $z = 0$. Assume that there is some $z_0 > 0$ such that $f_0(z) > z$ for all $z \in (0, z_0)$. Then for each $\epsilon > 0$ the smallest fixed point $\hat{z}$ of $f_\epsilon(z)$ will always be larger than z_0 (see Figure 4(a)) and the final fraction of infected nodes in the graph will w. h. p. be larger than $\mathbb{E}[\mathbb{P}(\mathrm{Poi}(W^- z_0) \geq T)])$. In particular, we derive the following theorem:

Theorem 2.12. *Assume that there is $z_0 > 0$ such that $f_0(z) > z$ for all $z \in (0, z_0)$. Then the system is non-resilient.*

The assumption of this theorem is satisfied in particular if f_0 has right derivative larger than 1 at $z = 0$. The remaing cases, see also Figure 4(b) for an illustration, are covered by the following result:

Theorem 2.13. *Assume that $f_0(z)$ is continuously differentiable from the right at $z = 0$ with derivative $f'_0(0) < 1$. Then the system is resilient.*

We again refer to [15] for a version of Theorem 2.13 which makes weaker but also more technical assumptions on f_0.



(a) (b)

Figure 4: Plot of the functions f_0 (dashed) and f_ϵ (solid) for $\epsilon > 0$, $T = 2$ and weights $W^- = W^+$ Pareto-distributed with shape parameter (a) 2.5 and (b) 3.5.

Let us now discuss some consequences of Theorems 2.12 and 2.13 in more detail. Let us make the technical assumption $\mathbb{E}[W^-W^+] < \infty$. This is of course always satisfied if W^-, W^+ are independent, but it also captures many other cases in which there are significant correlations between the in- and out-degrees of the nodes: a characteristic setting is for example when $W^- \approx W^+$, and then the condition guarantees that both W^-, W^+ have bounded second moment. Under the assumption $\mathbb{E}[W^-W^+] < \infty$ we get the explicit representation

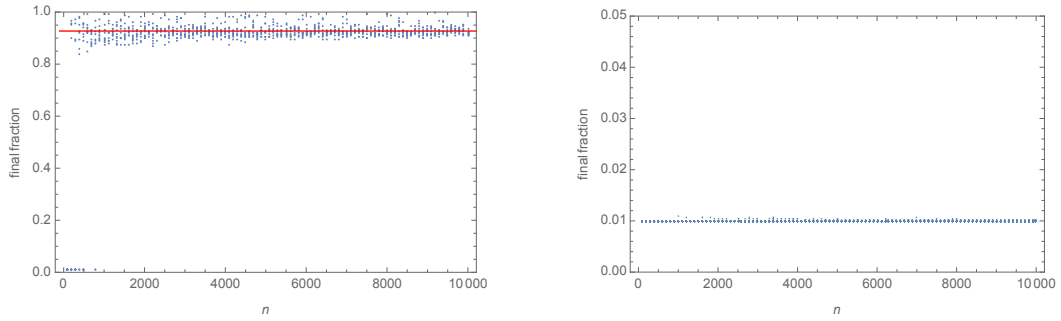
$$f_0'(z) = \mathbb{E}[W^-W^+\mathbb{P}(\mathrm{Poi}(W^-z) = T - 1)]$$

and this is continuous for $z \in [0, \infty)$. Hence Theorems 2.12 and 2.13 almost entirely characterize resilience in this case. In particular, if $T \geq 2$ almost surely, we get $f_0'(0) = 0$ and hence by Theorem 2.13 such networks are always resilient, which is consistent with our findings in the previous section. This readily yields sufficient requirements to make the system resilient.

However, note that the condition $\mathbb{E}[W^-W^+] < \infty$ is typically not satisfied for weights (i. e. degrees) with unbounded second moment which are frequently observed for real networks, such as interbank networks. It is then the case that also networks with $T \geq 2$ (or also $T \geq r$ for any $r \in \mathbb{N}$) almost surely can satisfy the condition in Theorem 2.12 and are hence non-resilient. See Figure 5(a) for simulations on networks of finite size with weights $W^- = W^+$ according to a Pareto distribution with shape parameter 2.5 (i. e. with finite first moment but infinite second moment) and constant threshold $T = 2$. The final fraction of infected nodes concentrates around the asymptotic lower bound of 92.7% and the networks are hence non-resilient (with exception of only a few networks of very small size).

While the non-resilience property might be a favorable one in some applications where a large coverage of the network is targeted, for many others, such as financial networks, resilience is the desirable property. A characterization of resilient and non-resilient networks also in the case that $\mathbb{E}[W^-W^+] = \infty$ is hence of high interest. The reason why $T \geq 2$ is not sufficient for resilience anymore is that there exist very strongly connected nodes in the network which either receive a lot of edges (have high in-weight) and are hence very susceptible or send a lot of edges (have high out-weight) and hence infect a large proportion of the network once they become infected. Typically in networks there are nodes which have both high in-weight and high out-weight which further increases the importance of their role in the infection process. Exactly these nodes are the ones that have to be equipped with higher thresholds when it comes to controlling systemic risk in the network.

Typically, as for example in the regulation of the financial sector, risk management strategies intend to ensure the survival of some given node by focusing on the risk exposures towards



(a) (b)

Figure 5: Scatter plot of the final infection fraction for 10^4 simulations of finite networks. Weights $w_i^- = w_i^+$ are drawn from a Pareto distribution with shape parameter 2.5 and initially 1% of all nodes are infected. The thresholds are given by (a) $\tau_i = 2$ respectively (b) $\tau_i = \max\{2, \alpha_c(w_i^-)^{\gamma_c}\}$. In (a), the red line marks the asymptotic lower bound on the final infection fraction of about 92.7%.

(i. e. infections from) other nodes and hence incoming links in the network. In this spirit we aim to state threshold requirements which depend on a node's in-weight. More precisely, we intend to characterize resilience/non-resilience properties for heterogeneous networks where the thresholds τ_i are given by $\tau(w_i^-)$ for some non-decreasing integer-valued function $\tau : \mathbb{R} \to \mathbb{N}$. This then allows for the management of systemic risk by deriving sufficient threshold requirements for each particular node simply by observing (estimating) the respective in-weight and plugging it into function τ.

We will see that the threshold requirements strongly depend on the tail of the weight distributions. What is typically observed for degree (weight) distributions of real networks is that they closely resemble Pareto distributions in their tail. We thus assume in the following that the weight distributions are Pareto distributions and refer to [16] for results on more general weight distributions. That is, there exist parameters $\beta^-, \beta^+ > 2$ (in order to ensure integrability of W^- and W^+) and minimal weights $w^-_{\min}$ and $w^+_{\min}$ such that the weight densities are given by

$$f_{W^\pm} = (\beta^\pm - 1)(w^\pm_{\min})^{\beta^\pm - 1} w^{-\beta^\pm} \mathbf{1}\{w \geq w^\pm_{\min}\}.$$

It will turn out that the quantities

$$\gamma_c := 2 + \frac{\beta^- - 1}{\beta^+ - 1} - \beta^- \quad \text{and} \quad \alpha_c := \frac{\beta^+ - 1}{\beta^+ - 2} w^+_{\min} (w^-_{\min})^{1-\gamma_c}$$

play a central role in determining sufficient threshold requirements. It holds that $\gamma_c < 0$ only if $\mathbb{E}[W^- W^+] < \infty$. In this case it is hence sufficient to require $\tau_i \geq 2$ for all $i \in [n]$ as has been discussed above. For all other cases, we investigate systems with $\tau_i \approx \alpha(w_i^-)^\gamma$ for certain constants α and γ.

Theorem 2.14. *Let the weights W^- and W^+ be Pareto distributed with parameters $\beta^-, \beta^+ > 2$ and $w^-_{min}, w^+_{min} > 0$ and assume that $\tau_i = \tau(w_i^-)$ for some function $\tau : \mathbb{R} \to \mathbb{N}\backslash\{1\}$. Then the system is resilient, if one of the following holds:*

1. *$\gamma_c < 0$,*
2. *$\gamma_c = 0$ and $\liminf_{w\to\infty} \tau(w) > \alpha_c + 1$,*

3. $\gamma_c > 0$ *and* $\liminf_{w\to\infty} w^{-\gamma_c}\tau(w) > \alpha_c$.

Note that Theorem 2.14 only derives sufficient requirements to make the system resilient. In [16], it is shown that these requirements are actually sharp in the sense that networks become non-resilient for thresholds $\tau_i = \tau(w_i^-)$ if τ satisfies $\limsup_{w\to\infty} w^{-\gamma_c}\tau(w) < \tilde{\alpha}_c$ for a certain $\tilde{\alpha}_c > 0$ which depends on the dependence structure between W^- and W^+. In the case that the weights are comonotone (nodes with larger in-weights also have larger out-weights and vice versa), $\tilde{\alpha}_c$ coincides with α_c from Theorem 2.14.

Moreover, Theorem 2.14 only ensures resilience in the limit $n \to \infty$ and $\epsilon \to 0$. The derived threshold requirements are, however, also applicable to reasonably sized finite networks with positive initial infection probability. See for example Figure 5(b) for simulations on networks with sizes in $[10^2, 10^4]$ and enforced threshold requirements $\tau_i = \max\{2, \alpha_c(w_i^-)^{\gamma_c}\}$ for all $i \in [n]$. The observed amplification is almost negligible. It is hence possible to implement risk management strategies based on Theorem 2.14 for real networks. Usually (if $\gamma_c > 0$) such strategies require larger (more connected) nodes to ensure higher resistance (threshold). However, since $\beta^-, \beta^+ > 2$, it holds that $\gamma_c < 1$ and the threshold function τ thus only needs to increase sublinearly with the weight. Finally, it is an appealing feature of our formula that for each node i the required threshold τ_i can be computed locally, i. e. only using information about its own edges once α_c and γ_c are known. This contrasts our risk management strategies from other approaches, where always knowledge about the entire system needed to be assumed.

2.3 A weighted contagion process

In the previous sections, the contagion process was always based on counting the number of infected neighbors. In the first step, a node became infected as soon as any of its neighbors became infected. Later, we allowed for $r \geq 2$ neighbors to default before a certain node became infected and finally we assigned to each node $i \in [n]$ an individual threshold value τ_i. For many applications, however, the mere counting of infected neighbors is not enough, since rather the *strength* of the links to these infected neighbors is the determining quantity. For instance, in an interbank network, it is not the number of defaulted loans but rather their total amount that is relevant for the infection process. In this section, we therefore enhance our previous model once more to account for weighted edges.

In the specification of the random graph, we model the occurrence of edges as before by (2.1). Additionally, we assign to each node $j \in [n]$ a sequence of possible exposures $E_{1,j}, \dots, E_{n,j}$ modeled by exchangeable $\mathbb{R}_+$-valued random variables, meaning that the order of the exposures does not influence their joint distribution. The random variable $E_{i,j}$ shall then describe a possible exposure from node i to node j. That is, we want to place it on an edge going from i to j if this edge is present in the graph. The assumption that the exposure list consists of exchangeable random variables is sensible for networks in which the strength of a link is determined by the receiving edge rather than by the sending edge (note that the exposure lists can significantly vary between different nodes $j \in [n]$).

In order to describe the contagion mechanism, we now assign to each node $i \in [n]$ an $\mathbb{R}_+$-valued parameter c_i resembling the strength of i. Motivated by the application to financial networks we will call c_i the capital of i hereafter. Similarly as previously we then describe the contagion process in the network as follows: At the beginning a fraction $\epsilon > 0$ of all nodes is infected. Other nodes in the network become infected as soon as their total exposure to infected nodes exceeds their capital. Note that our previous model is incorporated in this new model simply by choosing integer-valued capitals and $E_{i,j} = 1$ for all $i \neq j$. In this case, the capitals c_i had the interpretation of threshold values. In analogy to the previous model, we therefore introduce for each node $i \in [n]$ a threshold value τ_i which shall count the number of neighbors

that can cause the infection of i. To be more precise, τ_i shall be the smallest integer value such that $\sum_{\ell \leq \tau_i} E_{\ell,i} \geq c_i$ if such a value exists. If $\sum_{\ell=1}^{n} E_{\ell,i} < c_i$, we simply set $\tau_i = \infty$. Then τ_i is a random variable and it only describes a *hypothetical* threshold value since usually the nodes will not become infected in their natural order during the infection process. We now assume that still in the limit when the network size $n \to \infty$ the thresholds are described by a random variable T. Then due to exchangeability of the exposure random variables and large network effects we can restate Theorem 2.11 for this new model, where again

$$f_\epsilon(z) := \epsilon \mathbb{E}[W^+] + (1-\epsilon)\mathbb{E}[W^+ \mathbb{P}(\mathrm{Poi}(W^- \hat{z}) \geq T)].$$

Theorem 2.15. *Let $\hat{z}$ be the smallest fixed point of f_ϵ and assume that it is stable. Then, the fraction of eventually infected nodes converges in probability to*

$$\alpha(\epsilon) = \epsilon + (1-\epsilon)\mathbb{E}[\mathbb{P}(\mathrm{Poi}(W^- \hat{z}) \geq T)].$$

Also the results about non-resilience and resilience of the network generalize to the more complex setting.

Theorem 2.16. *Assume that there is $z_0 > 0$ such that $f_0(z) > z$ for all $z \in (0, z_0)$. Then the system non-resilient.*

Theorem 2.17. *Assume that $f_0(z)$ is continuously differentiable from the right at $z = 0$ with derivative $f_0'(0) < 1$. Then the network is resilient.*

Finally, under some rather mild assumptions on the exposure sequences such as $\mathbb{E}[E_{j,i}] = \mu_i$ for all $j \in [n]$, we can also reformulate Theorem 2.14 for the new model which equips us with a formula for sufficient capital requirements to secure a system. See [16] for a precise formulation of Theorem 2.18 and its assumptions.

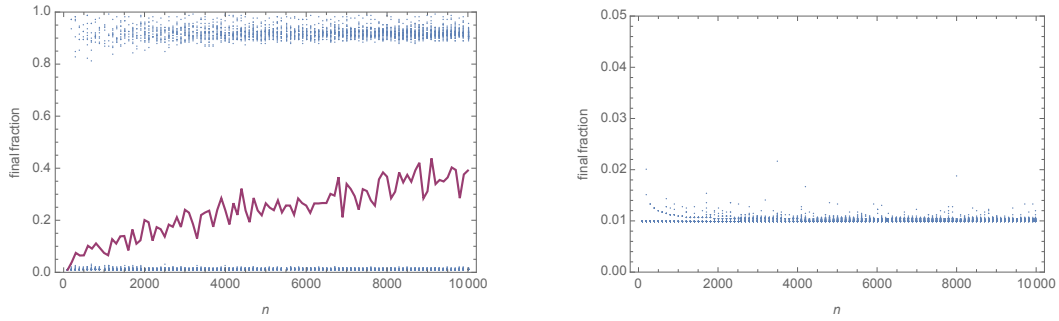
Theorem 2.18. *Let the weights W^- and W^+ be Pareto distributed with parameters $\beta^-, \beta^+ > 2$ and $w^-_{min}, w^+_{min} > 0$. Further assume that $c_i > \max_{j \in [n]} E_{j,i}$ (the capital is larger than the largest exposure) almost surely for all $i \in [n]$. Then the following holds:*

1. *If $\gamma_c < 0$, then the system is resilient.*

If additionally, there exists a function $\tau : \mathbb{R} \to \mathbb{N}$ such that the capitals satisfy $c_i \geq \tau(w_i^-)\mu_i$ almost surely for all $i \in [n]$, then the system is resilient if one of the following holds:

2. *$\gamma_c = 0$ and $\liminf_{w \to \infty} w^{-\gamma} \tau(w) > 0$ for some $\gamma > 0$,*
3. *$\gamma_c > 0$ and $\liminf_{w \to \infty} w^{-\gamma_c} \tau(w) > \alpha_c$.*

In particular, in the usual case that $\gamma_c > 0$ (for example $\beta^-, \beta^+ < 3$) Theorem 2.18 ensures resilience if each institution i holds capital larger than $\alpha_c (w_i^-)^{\gamma_c} \mu_i$ (and not less than its largest exposure). As before, this is a quantity that can be computed by each institution individually simply by counting and averaging their exposures in the system. The theorem hence provides us with an easy applicable risk management policy to prevent networks from systemic risk. To test its applicability we pursue simulations similar to the ones from Figures 5(a) and 5(b) but enrich the network with Pareto distributed exposures with shape parameter 2.5. As can be seen from Figure 6(a) it is not sufficient to only prohibit contagious links in the network in order to make the system resilient. The derived capital requirements from Theorem 2.18 on the other hand ensure resilience of the system as can be seen from Figure 6(b). Note that the outcome of the simulation is more volatile than for the threshold model from Section 2.2 since also the exposure sizes carry a lot of randomness. Still our derived capital requirements work very well to contain the infection.



(a) (b)

Figure 6: Scatter plot of the final infection fraction for 10^4 simulations of finite weighted networks. Node-weights $w_i^- = w_i^+$ are drawn from a Pareto distribution with shape parameter 2.5 as are the edge-weights $E_{j,i}$, and initially 1% of all nodes are infected. The capitals are given by (a) $c_i = 1.001 \max_{j\in[n]} E_{j,i}$ respectively (b) $c_i = \max\{1.001 \max_{j\in[n]} E_{j,i}, \alpha_c (w_i^-)^{\gamma_c} \mu_i\}$. In (a), the red line marks the average final fraction over all 100 simulations for each network size.

References

[1] N. Alon and J. H. Spencer. *The Probabilistic Method*. Wiley Publishing, 4th edition, 2016.

[2] H. Amini, R. Cont, and A. Minca. Resilience to Contagion in Financial Networks. *Mathematical Finance*, 26(2):329–365, 2016.

[3] H. Amini, D. Filipović, and A. Minca. Systemic Risk and Central Clearing Counterparty Design. *Swiss Finance Institute Research Paper*, pages 13–34, 2015.

[4] H. Amini and N. Fountoulakis. Bootstrap Percolation in Power-Law Random Graphs. *Journal of Statistical Physics*, 155(1):72–92, 2014.

[5] H. Amini, N. Fountoulakis, and K. Panagiotou. Bootstrap Percolation in Inhomogeneous Random Graphs. *arXiv:1402.2815*, 2014.

[6] Y. Armenti, S. Crépey, S. Drapeau, and A. Papapantoleon. Multivariate Shortfall Risk Allocation and Systemic Risk. *SIAM Journal on Financial Mathematics*, 9(1):90–126, 2018.

[7] P. Artzner, F. Delbaen, J. Eber, and D. Heath. Coherent Measures of Risk. *Mathematical Finance*, 9(3):203–228, 1999.

[8] F. Biagini, J.-P. Fouque, M. Fritelli, and T. Meyer-Brandis. A Unified Approach to Systemic Risk Measures via Acceptance Sets. *Mathematical Finance*, Forthcoming.

[9] B. Bollobás. *Random Graphs*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2001.

[10] J. Chalupa, P. L. Leath, and G. R. Reich. Bootstrap Percolation on a Bethe Lattice. *Journal of Physics C: Solid State Physics*, 12(1):L31–L35, 1979.

[11] C. Chen, G. Iyengar, and C. Moallemi. An Axiomatic Approach to Systemic Risk. *Management Science*, 59(6):1373–1388, 2013.

[12] C. Chong and C. Klüppelberg. Contagion in Financial Systems: A Bayesian Network Approach. *SIAM Journal on Financial Mathematics*, 9(1):28–53, 2018.

[13] F. Chung and L. Lu. Connected Components in Random Graphs with Given Expected Degree Sequences. *Annals of Combinatorics*, 6(2):125–145, 2002.

[14] F. Chung and L. Lu. The Average Distances In Random Graphs With Given Expected Degrees. *Internet Mathematics*, 1:91–114, 2003.

[15] N. Detering, T. Meyer-Brandis, and K. Panagiotou. Bootstrap Percolation in Directed and Inhomogeneous Random Graphs. *arXiv:1511.07993*, 2016.

[16] N. Detering, T. Meyer-Brandis, K. Panagiotou, and D. Ritter. Managing Default Contagion in Inhomogeneous Financial Networks. *arXiv:1610.09542*, 2017.

[17] L. Eisenberg and T. H. Noe. Systemic Risk in Financial Systems. *Management Science*, 47(2):236–249, 2001.

[18] P. Erdös and A. Rényi. On the evolution of random graphs. In *PUBLICATION OF THE MATHEMATICAL INSTITUTE OF THE HUNGARIAN ACADEMY OF SCIENCES*, pages 17–61, 1960.

[19] Z. Feinstein, B. Rudloff, and S. Weber. Measures of Systemic Risk. *SIAM Journal on Financial Mathematics*, 8(1):672–708, 2017.

[20] J.-P. Fouque and J. A. Langsam, editors. *Handbook on systemic risk*. Cambridge University Press, Cambridge, 2013.

[21] P. Gai and S. Kapadia. Contagion in Financial Networks. *Proceedings of the Royal Society A*, 466:2401–2423, 2010.

[22] A. Gandy and L. A. M. Veraart. A Bayesian Methodology for Systemic Risk Assessment in Financial Networks. *Management Science*, 63(12):4428–4446, 2017.

[23] E. N. Gilbert. Random Graphs. *Ann. Math. Statist.*, 30(4):1141–1144, 1959.

[24] H. Hoffmann, T. Meyer-Brandis, and G. Svindland. Risk-Consistent Conditional Systemic Risk Measures. *Stochastic Processes and their Applications*, 126(7):2014–2037, 2016.

[25] H. Hoffmann, T. Meyer-Brandis, and G. Svindland. Strongly Consistent Multivariate Conditional Risk Measures. *Mathematics and Financial Economics*, DOI 10.1007/s11579-017-0210-3, 2018.

[26] R. v. d. Hofstad. *Random Graphs and Complex Networks*, volume 1 of *Cambridge Series in Statistical and Probabilistic Mathematics*. Cambridge University Press, 2016.

[27] T. R. Hurd. *Contagion! Systemic Risk in Financial Networks*. Springer, 2016.

[28] S. Janson, T. Luczak, and A. Rucinski. *Random Graphs*. Wiley Series in Discrete Mathematics and Optimization. Wiley, 2011.

[29] S. Janson, T. Łuczak, T. Turova, and T. Vallier. Bootstrap Percolation on the Random Graph $G_{n,p}$. *Ann. Appl. Probab.*, 22(5):1989–2047, 10 2012.

[30] E. Kromer, L. Overbeck, and K. Zilch. Systemic Risk Measures on General Measurable Spaces. *Mathematical Methods of Operations Research*, 84(2):323–357, 2016.

[31] M. Kusnetsov and L. A. M. Veraart. Interbank Clearing in Financial Networks with Multiple Maturities. *Preprint*, 2016.

[32] S. Weber and S. Weske. The Joint Impact of Bankruptcy Costs, Cross-Holdings and Fire Sales on Systemic Risk in Financial Networks. *Probability, Uncertainty and Quantitative Risk*, 2(9):1–38, 2017.